

REMARKS

This Amendment after Final is filed in response to the Final Office Action mailed Dec. 10, 2007. The Applicant respectfully urges the application is in condition for allowance. To the extent that any objections or rejections may still be applicable they are respectfully traversed.

Claims 1-25 are pending in the case.

Claims 1, 18 and 19 have been amended to include indicated allowable subject matter. The Applicant respectfully urges that entry of these amendments is appropriate after final, as it will advance the prosecution of the case and avoid undue delays.

No new claims have been added

Response to Examiner's Response to Arguments

At paragraph 5 of the Office Action, the Examiner agreed that claim 11 was allowable, indicating that the claimed "a system controller with a HWA module to discard malicious packets before it can be forwarded to the CPU" was not shown by the prior art.

The Applicant has amended claims 1, 18 and 19 to include the indicated allowable subject matter of claim 11. Specifically, the claims now recite that the discarding is by/at "a hardware assist (HWA) module of a system controller that is coupled to the CPU." Accordingly, the Applicant respectfully urges such claims are allowable and requests issue of a notice of allowance.

Claim Rejections - 35 U.S.C. §103

At paragraphs 1-2 of the Office Action, claims 1-4, 9, 10, 18 and 19 were rejected under 35 U.S.C. §103(a) over Viswanath et al., U.S. Patent No. 6,950,435 (hereinafter "Viswanath"), in view of Milliken, U.S. Patent Publication No. 2003/0115485 (hereinafter "Milliken").

The Applicant's claim 1, representative in part of the other rejected claims, sets forth (emphasis added):

1. (CURRENTLY AMENDED) A method for a network node, which includes a central processing unit (CPU) configured to execute a router operating system, to filter malicious data packets received at the network node, the method comprising:

- receiving a data packet at the network node;
- performing hash-based flow classification on the received data packet to determine whether the received data packet is a malicious data packet; and

discarding, by a hardware assist (HWA) module of a system controller that is coupled to the CPU, the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.

Viswanath discusses a switch with a switching fabric (Fig. 1, 25) that makes “frame forwarding decisions for received packets.” *See* col. 4, lines 41-43. A flow module (Fig. 2, 44) generates hash keys based on addresses and port numbers of received packets and combines these keys to form a packet signature. *See* Fig. 4, 74. The flow module then searches a signature table and if there is a match, forwards an entry to the switching fabric, the entry for use in executing a switching decision. *See* col. 8, lines 29-34.

Milliken discusses a security router where a “[h]ash processor 310 may optionally compare generated hash value(s) to hash values of known viruses and/or worms within hash memory (320).” *See* paragraph 0060 and Fig. 5, 515. “If one or more of the generated hash values match one of the hash values of known viruses and/or worms, the hash processor may take remedial actions...[such as] dropping the packet.” *See* paragraph 0060 and Fig. 5, 550.

The Applicant respectfully urges that the combination of Viswanath and Milliken does not teach or suggest the Applicant’s claimed “***discarding, by a hardware assist (HWA) module of a system controller that is coupled to the CPU, the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.***”

In contrast to prior techniques that have consumed CPU processing bandwidth identifying and removing malicious packets from a system memory, the Applicant claims **discarding, by a hardware assist (HWA) module of a system controller that is coupled to the CPU, the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet.** As the CPU is not burdened by removing such packets, the system is less susceptible to, for example, denial-of-service attacks designed to disrupt network communication by overburdening a CPU.

The Examiner agrees that Viswanath does not discuss discarding malicious packets. As such, Viswanath clearly cannot suggest discarding packets by a special HWA module that operates on packets before a malicious data packet is forwarded to the CPU.

Milliken does discuss discarding packets, but does not suggest one should do so in the manner the Applicant claims. Rather than employ **a hardware assist (HWA) module of a system controller that is coupled to the CPU,** Milliken simply describes a hash processor between input and output ports. See Fig. 3. Thus, Milliken does not appear to suggest **discarding, by a hardware assist (HWA) module of a system controller that is coupled to the CPU, the received data packet before the data packet can be forwarded to the CPU for processing,** rather than discarding by a CPU as is typically done.

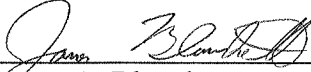
Accordingly, the Applicant respectfully requests reconsideration of the rejection and urges that Viswanath and Milliken are insufficient to make obvious the present claims under 35 U.S.C. §103 because of the absence of the Applicant's claimed novel **"discarding, by a hardware assist (HWA) module of a system controller that is coupled to the CPU, the received data packet before the data packet can be forwarded to the CPU for processing by the router operating system, if the received data packet is determined to be a malicious data packet."**

Should the Examiner believe there are any remain issues that may delay a Notice of Allowance the Examiner is invited to telephonically contact the undersigned attorney at (617) 951-2500, in hopes any such issues may be resolved in an expedited manner.

In summary, all the independent claims are believed to be in condition for allowance and therefore all dependent claims that depend there from are believed to be in condition for allowance. The Applicant respectfully solicits favorable action.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,



James A. Blanchette
Reg. No. 51,477
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500